Περραιβού 40, Άνω Τούμπα
54352, Θεσσαλονίκη
W: www.servicepack.gr
T: 2310.943.054
M: 6978.284.405
E: info@servicepack.gr

Προστασία Δεδομένων

Πιθανά Προβλήματα

Πρόληψη - Αντιμετώπιση

Αγαπητοί πελάτες και συνεργάτες,

Κινούμενοι συνεχώς με γνώμονα την ικανοποίηση των πελατών μας και την εύρυθμη λειτουργία των επιχειρήσεών τους, θα θέλαμε να σας ενημερώσουμε **για την προστασία των δεδομένων.**

Όλες οι επιχειρήσεις σήμερα καταγράφουν και επεξεργάζονται δεδομένα με σκοπό την εξαγωγή απαραίτητης πληροφορίας για τη λειτουργία τους. Είναι ευθύνη κάθε επιχείρησης να έχει ολοκληρωμένη πολιτική για την προστασία των δεδομένων και των συστημάτων της, διότι σε περίπτωση απώλειας των δεδομένων της, διακινδυνεύει τη λειτουργία και την επιβίωσή της.

Ποια είναι τα κρίσιμα δεδομένα

Κρίσιμα για τη λειτουργία της επιχείρησης δεν είναι μόνο αρχεία δεδομένων, αλλά επίσης: το λειτουργικό σύστημα, οι ρυθμίσεις του συστήματος και το λογισμικό που είναι εγκατεστημένο στον server ή client. Πιο αναλυτικά στα παραπάνω μπορεί να περιλαμβάνονται:

- Λειτουργικά συστήματα και άδειες χρήσης
- Ρυθμίσεις συστήματος (π.χ. boot sector, δομή partition δίσκου, ρυθμίσεις δικτύου κλπ)
- Metadata συστήματος (π.χ. registry)
- Εγκατεστημένα προγράμματα με τις άδειες χρήσης τους
- Δεδομένα προγραμμάτων (σε αρχεία ή βάση δεδομένων)
- Αρχεία επιχειρησιακών εγγράφων (όπως Word, Excel, PDF) που τηρούμε (π.χ. ολόκληρος ο φάκελος documents and settings)
- Αρχεία σε άλλους φακέλους του χρήστη (π.χ. downloads)
- Φωτογραφίες και αρχεία ήχου
- Αρχεία mails από πρόγραμμα διαχείρισης ηλεκτρονικού ταχυδρομείου
- Ρυθμίσεις λογαριασμού ηλεκτρονικού ταχυδρομείου
- Προγράμματα οδήγησης οποιαδήποτε περιφερειακής συσκευής (φορολογικός μηχανισμός, εκτυπωτής, barcode reader, ζυγαριά κ.α.)
- Metadata αρχείων όπως δεδομένα δικαιωμάτων, ιδιοκτητών, ομάδων κλπ.
- Ό,τι άλλο προκύπτει από τη λειτουργία μιας θέσης εργασίας.

Δεδομένα και απειλές

Τα δεδομένα συνήθως αποθηκεύονται σε σκληρούς δίσκους εντός της επιχείρησης. Οι βασικοί κίνδυνοι που απειλούν τους σκληρούς δίσκους και κατ' επέκταση, τα δεδομένα είναι:

1. **Φυσιολογική φθορά** από τη χρήση του σκληρού δίσκου, η οποία μειώνει τη διάρκεια ζωής του.
2. **Βλάβη** στο σκληρό δίσκο (π.χ. από κραδασμό).
3. **Μεταπτώσεις τάσης, διακοπές ρεύματος** κτλ, με αποτέλεσμα προβλήματα στη λειτουργία και μείωση χρόνου ζωής ή ακόμα και καταστροφή του σκληρού δίσκου. Ο παραπάνω κίνδυνος φυσικά υφίσταται για **το σύνολο του hardware** (κάρτες δικτύου, μητρική κάρτα, τροφοδοτικό κ.α.) ενός υπολογιστή.
4. **Φυσική καταστροφή όπως πλημμύρα, φωτιά κλπ στο χώρο εργασίας**, με αποτέλεσμα την καταστροφή μηχανημάτων και δεδομένων.
5. **Κλοπή** μέρους ή του συνόλου του μηχανολογικού εξοπλισμού της επιχείρησης.

Τα παραπάνω αποτελούν ενδεικτικές περιπτώσεις φυσικής φθοράς (Hardware Failure). Εδώ πρέπει να προσθέσουμε και το ανθρώπινο λάθος ή τα προβλήματα λογισμικού (Software Failure). Ενδεικτικά, αναφέρουμε την μόλυνση από ιούς, " έσβησα το αρχείο κατά λάθος" κ.α.

Αντίκτυπος στην επιχείρηση

Σε περίπτωση που λάβει χώρα κάποια από τις παραπάνω περιπτώσεις και **δεν έχει προετοιμαστεί κατάλληλα η επιχείρηση,** είναι επόμενο να προκύψουν εμπόδια στη λειτουργία της. Αυτό επιφέρει με τη σειρά του **οικονομικό κόστος** στο οποίο πρέπει να συμπεριληφθεί επίσης **το κόστος αποκατάστασης της όποιας βλάβης** έχει συμβεί. Επιπλέον ο χρόνος επαναφοράς των δεδομένων και των συστημάτων δεν μπορεί να υπολογιστεί.

Ενδεικτικά παρατίθεται ένα παράδειγμα:

Σενάριο: Καίγεται ο σκληρός δίσκος σε ένα από τα τερματικά (π.χ. ταμείο) της επιχείρησης

- η θέση εργασίας παύει να λειτουργεί έως ότου αποκατασταθεί
- το άτομο που απασχολούνταν εκεί, μένει ανενεργό ή εργάζεται επιβαρύνοντας το χρόνο και χώρο άλλου ατόμου
- παραγγελία και παραλαβή/ άμεση αγορά προϊόντος για αποκατάσταση τερματικού.
- μίσθωση και σχετική διαθεσιμότητα τεχνικού συνεργάτη για την αποκατάσταση του τερματικού (εγκατάσταση Windows, εφαρμογών και προγραμμάτων, περιφερειακών συσκευών, διαμόρφωση ρυθμίσεων κ.τ.λ.)
- επαναφορά τοπικών δεδομένων/ ρυθμίσεων (σε περίπτωση ύπαρξης εφεδρικού αντιγράφου ασφαλείας) ή ολική απώλεια

Από ένα απλό παράδειγμα βλέπουμε ότι ο χρόνος επαναλειτουργίας του τερματικού είναι τουλάχιστον μια- δυο ημέρες, χωρίς να υπολογίσουμε το χρόνο παραλαβής του υλικού, τη διαθεσιμότητα του τεχνικού κ.ά.

Τρόποι πρόληψης

Τις **απειλές** που αναφέρθηκαν μπορούμε να τις **αντιμετωπίσουμε** με τους παρακάτω τρόπους, ώστε το **downtime της επιχείρησης** σε κάθε περίπτωση **να είναι το λιγότερο δυνατό.**

1. **Για την επίλυση του θέματος των μεταπτώσεων – διακοπών τάσης, προτείνεται η χρήση UPS.** Το UPS διασφαλίζει τη λειτουργία του Η/Υ με επαρκή χρονική διάρκεια σε περίπτωση διακοπής ρεύματος, ώστε να μπορέσει ο χρήστης να κάνει ασφαλή τερματισμό λειτουργίας. Ακόμη πιο κρίσιμο είναι το γεγονός ότι λειτουργεί **ως σταθεροποιητής τάσης** και εξασφαλίζει τη συνεχή λειτουργία του Η/Υ και των περιφερειακών του με σταθερή παροχή τάσης. **Συνδέουμε στο UPS οποιαδήποτε περιφερειακή συσκευή** (φορολογικός μηχανισμός, εκτυπωτής, barcode reader κ.α.) είναι σημαντική για τη λειτουργία της επιχείρησης.
2. **Για την επίλυση προβλημάτων σχετικά με απώλεια δεδομένων, προτείνεται η καθημερινή λήψη backup** ώστε να υπάρχει η πιο πρόσφατη εικόνα διαθέσιμη.

   <u>Μεθοδολογίες backup</u>

   Backup μπορεί να ληφθεί με πολλούς διαφορετικούς τρόπους. Ενδεικτικά αναφέρουμε:

   - **1η μεθοδολογία λήψης Backup που συνήθως πραγματοποιούν όσοι χρησιμοποιούν κάποιο πρόγραμμα που αποθηκεύει δεδομένα σε βάση δεδομένων (Database Backup):**

   - **Backup της βάσης με το αυτόματο σύστημα backup του SQL server.** Σε περίπτωση που δε γίνεται να λάβει backup ο SQL Server αυτόματα (π.χ. στην Express έκδοση), τότε γίνεται χρονοπρογραμματισμός της εργασίας από το αντίστοιχο εργαλείο των Windows.
     Εναλλακτικά, μπορεί να γίνει **χειροκίνητα** από κάποιο χρήστη. Τονίζεται ότι συμπεριλαμβάνουμε στη διαδικασία backup **όλες τις βάσεις** που υφίστανται στον SQL Server.
     Η συγκεκριμένη μεθοδολογία δεν είναι ιδανική γιατί:
     1. σε περίπτωση χειροκίνητου backup, δεν είμαστε σίγουροι ότι ο χρήστης θα θυμάται να εκτελεί τη διαδικασία τακτικά
     2. ακόμα και σε περίπτωση αυτόματου backup, περιλαμβάνεται μόνο η βάση ή οι βάσεις δεδομένων και όχι τα υπόλοιπα σημαντικά δεδομένα.

Τι πρέπει να προσέχουμε εάν λαμβάνουμε backup (χειροκίνητο ή αυτόματο) της βάσης:

1. **Βεβαιωθείτε ότι το backup που λαμβάνεται είναι της σωστής βάσης (και χρονιάς).** Υπάρχουν πολλές περιπτώσεις συστημάτων, όπου κάθε νέο έτος αλλάζει η βάση που χρησιμοποιείται. Εκεί η προγραμματισμένη διαδικασία backup χρειάζεται τροποποίηση για να μη βλέπει την προηγούμενη βάση.
2. **Βεβαιωθείτε ότι το αρχείο backup λειτουργεί και μπορεί να επαναφέρει τη βάση απροβλημάτιστα, αλλιώς είναι άχρηστο.** Αυτό γιατί μπορεί ένα αρχείο να μην έχει εξαχθεί σωστά (corrupted file) ή να μην έχει ολοκληρωθεί επειδή διακόπηκε η διαδικασία εξαγωγής του (incomplete file).
3. **Βεβαιωθείτε ότι λαμβάνετε ξεχωριστό backup από όλα τα σημαντικά δεδομένα πέρα από τη βάση δεδομένων του προγράμματος σας.** Όπως προαναφέρθηκε, σημαντικά επίσης είναι διάφορα άλλα **files (documents, e-mails, ρυθμίσεις, drivers συσκευών, άδειες χρήσης κτλ.)**

Με τα παραπάνω κατά νου, προχωράμε στην επόμενη μεθοδολογία, η οποία λύνει τα περισσότερα θέματα με ιδανικότερο τρόπο.

- **2η μεθοδολογία λήψης Backup (Image Backup):**
  σύστημα image backup είτε σε εξωτερικό, δικτυακό ή μη, είτε σε εσωτερικό δεύτερο σκληρό δίσκο. Ο συγκεκριμένος τρόπος λαμβάνει την ακριβή εικόνα που έχει ο σκληρός δίσκος με **δεδομένα, λειτουργικό σύστημα, εφαρμογές εκείνη τη χρονική στιγμή.** Όταν επαναφέρουμε το image, ελαττώνεται σημαντικά ο χρόνος downtime.

  Προτείνουμε το Symantec Backup Exec System Recovery, το οποίο δίνεται μαζί με το Symantec Endpoint Protection Small Business Edition για ολοκληρωμένη προστασία antivirus και backup του image. Επιτελεί τη διαδικασία backup με ιδανικό τρόπο: λαμβάνει αρχικά ένα πλήρες Image του σκληρού δίσκου, ενώ στη συνέχεια κρατάει μόνο τις διάφορες αλλαγές στα δεδομένα σε σχέση με το αρχικό (differential backup).

  Σαφώς υπάρχει πλήθος εναλλακτικών προτάσεων για προγράμματα που εκτελούν αυτή τη διαδικασία, εκ των οποίων ένα από αυτά είναι και η λειτουργία αντίγραφου ασφαλείας (αρχείου ή και ειδώλου συστήματος) των Windows με τη δυνατότητα χρονοπρογραμματισμού.

Local ή offsite backup

Αναφέραμε νωρίτερα ότι το backup αποθηκεύεται σε εξωτερικό, δικτυακό ή μη, δίσκο είτε σε εσωτερικό δεύτερο σκληρό δίσκο. Επίσης, είναι συνηθισμένη τακτική να λαμβάνεται το backup στον ίδιο εσωτερικό δίσκο. **Καμία από αυτές τις λύσεις όμως δε διασφαλίζει την ασφάλεια των δεδομένων μας γιατί σε περίπτωση φυσικής καταστροφής, κλοπής κτλ. δε σώζουμε τίποτα.**
Χαρακτηριστικό παράδειγμα σεναρίου: πέφτει κεραυνός και) χτυπάει το δίκτυο με αποτέλεσμα να καούν όλα τα συνδεμένα μηχανήματα. Η λειτουργία της επιχείρησης

παύει έως ότου αποκατασταθεί η συνολική βλάβη, πράγμα που μπορεί να διαρκέσει πολύ μεγάλο χρονικό διάστημα!

Προτείνουμε τη λήψη και αποθήκευση image backup μέσω Symantec Backup Exec System Recovery σε NAS (Network Attached Storage) με ταυτόχρονη αντιγραφή σε δεύτερο σκληρό δίσκο, π.χ. σε άλλη τοποθεσία της επιχείρησης, στο cloud ή πολύ απλά σε εξωτερικό σκληρό δίσκο USB. Στην τελευταία περίπτωση, **συνετό είναι να παίρνουμε τον εξωτερικό σκληρό δίσκο και να τον απομακρύνουμε από την επιχείρηση,** αφού εκτελεστεί η διαδικασία λήψης backup.

Αποθήκευση παραπάνω του ενός backup

Δε θέλουμε να έχουμε μόνο το backup της τελευταίας ημέρας,**ώστε να έχουμε τη δυνατότητα roll-back σε προηγούμενης ημερομηνίας κατάσταση,** σε περίπτωση που στο πιο πρόσφατο έχουν συμπεριληφθεί σφάλματα, αλλαγές που δεν έχουν το επιθυμητό αποτέλεσμα κτλ.

Αυτό μπορεί να λειτουργήσει με τη χρήση δύο διαφορετικών εξωτερικών σκληρών δίσκων, όπου φέρνουμε εναλλάξ στην επιχείρηση για τη λήψη του backup στο τέλος της ημέρας: μια μέρα τον έναν και μια μέρα τον άλλο. Έτσι σε οποιαδήποτε βλάβη, θα έχουμε τη δυνατότητα επαναφοράς σε ημερομηνία το πολύ μίας ή δύο ημερών πριν τη βλάβη. Ακόμη θετικό είναι το γεγονός ότι σε περίπτωση βλάβης του ενός μέσου αποθήκευσης, συνεχίζουμε με ένα δεύτερο.

Χρήση RAID

Ολοκληρώνοντας την πρόταση μας για ολοκληρωμένη πολιτική προστασίας των δεδομένων, προτείνουμε τη χρήση των τεχνολογιών RAID 1 & RAID 1+0 στο server.

Το σύστημα RAID περιλαμβάνει τη συνδεσμολογία δύο σκληρών δίσκων (ή και παραπάνω) και τη χρήση μεθόδων όπως το striping (εγγραφή των δεδομένων σειριακά μία στον ένα δίσκο και μία στο δεύτερο), mirroring (ακριβής και ανά τακτά διαστήματα αντιγραφή του image του πρώτου σκληρού δίσκου στο δεύτερο) και ισοτιμία (μέθοδος με bit ισοτιμίας). Το σύστημα RAID στοχεύει στο να είναι πιο ασφαλές και πιο έμπιστο το σύστημα αποθήκευσης που εφαρμόζει η επιχείρηση.

Το RAID 1 αποτελείται από ένα σετ δύο δίσκων, από τους οποίους ο δεύτερος είναι ακριβές αντίγραφο του πρώτου. Αυτό το σύστημα χρησιμοποιείται όταν η ασφάλεια και η ταχύτητα ανάγνωσης των δεδομένων έχουν μεγαλύτερη βαρύτητα από ότι το μέγεθος του χώρου που υπάρχει διαθέσιμο για αποθήκευση δεδομένων. Αυτό μας βοηθάει στην περίπτωση που χαλάσει ένας δίσκος, συνεχίζει ο server τη λειτουργία του προσωρινά με το δεύτερο έως ότου γίνει αντικατάσταση. Το σετ δίσκων διαχειρίζεται από ένα controller, ο οποίος εάν πάθει κάποια βλάβη παύει η λειτουργία του RAID στο σύνολό του.

Το RAID 1+0 (δέκα) είναι μια πιο γρήγορη λύση από το RAID 1. Ισχύουν οι ίδιες αρχές και σε αυτή τη περίπτωση έχουμε δύο σετ δίσκων, όπου το δεύτερο σετ

είναι mirror του πρώτου. Για να μπορεί να αντικατασταθεί άμεσα ο χαλασμένος δίσκος, χρειάζεται να υπάρχει διαθέσιμος ένας ίδιος δίσκος. Οπότε προτείνεται κατά την επιλογή RAID συστήματος, να παίρνουμε ένα ή δύο ακόμη σκληρούς δίσκους ως ρεζέρβα, γιατί μπορεί άλλη χρονική στιγμή να μην είναι διαθέσιμος ίδιος δίσκος στην αγορά.

Επισημαίνουμε ότι η τεχνολογία RAID από μόνη της δεν αρκεί, καθώς δεν προστατεύει σε περίπτωση φωτιάς, κλοπής κλπ., οπότε προτείνεται επικουρικά στις προαναφερθείσες πρακτικές.

Για οποιαδήποτε απορία, είμαστε στη διάθεσή σας. Ευχαριστούμε για την προτίμηση και τη στήριξή σας.

Με εκτίμηση,